WHAT IS CLAIMED IS:

1. A data storage device comprising:

a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which each have a predetermined data capacity; and

cryptosystem means;

wherein said cryptosystem means receives, as cryptosystem keys for performing cryptosystem processing on data to be stored in said data storage area, a set of keys correlated with the encryption keys or decryption keys for each of the sectors from a device capable of performing data communication with said data storage device, and transmits, to said device, a set of encrypted keys obtained by executing encryption processing in the cipher block chaining (CBC) mode on the received set of keys.

2. A data storage device according to Claim 1, wherein said cryptosystem means generates key data as the header information of the data to be stored in said data storage area by using a storage key which is unique to said data storage device to execute the encryption processing in the CBC mode on the received set of keys.

3. A data storage device according to Claim 1,

wherein:

said data storage device performs mutual authentication with said device capable of performing data communication with said data storage device;

the received set of keys is a set of session-key-used CBC-mode-processing keys encrypted in the CBC mode by using a session key generated in the mutual authentication;

said cryptosystem means performs the decryption in the CBC mode of said set of encrypted session-key-used CBC-mode-processing keys; and

in said cryptosystem means, a set of storage-key-used CBC-mode-processing keys is generated by executing, based on a storage key unique to said data storage device, the encryption processing in the CBC mode on the set of decrypted session-key-used CBC-mode-processing keys, and said set of storage-key-used CBC-mode-processing keys is transmitted as header-information-forming data to said device.

4. A data storage device according to Claim 1, wherein:

said data storage device performs mutual authentication with said device capable of performing data communication with said data storage device;

the received set of keys is header information on the

data to be stored in said data storage area, and is a set of storage-key-used CBC-mode-processing keys encrypted in the CBC mode based on a storage key unique to said data storage device;

said cryptosystem means performs the decryption in the CBC mode of the set of encrypted storage-key-used CBC-mode-processing keys by using said storage key; and

in said cryptosystem means, a set of session-key-used CBC-mode-processing keys is generated by executing, based on a session key generated in the mutual authentication, the encryption processing in the CBC mode, and said set of session-key-used CBC-mode-processing keys is transmitted as data constituting decrypting key information.

5. A data storage device according to Claim 1, wherein:

from said device capable of performing data communication with said data storage device, said cryptosystem means receives: said set of keys correlated with the encryption keys or decryption keys for the sectors, as cryptosystem keys for performing cryptosystem processing on the data to be stored in said data storage area; and an integrity-check-value generating key of data to be stored in at least one of the sectors; and

in said cryptosystem means, the received set of keys

are encrypted in the CBC mode and are transmitted to said device.

6. A data recording method for a data processor comprising: a data storage device comprising cryptosystem means and a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which each have a predetermined data capacity; and a data recording device for executing data storage processing by transmitting data to said data storage device, said data recording method comprising the steps of:

executing mutual authentication processing between said data storage device and said data recording device;

when the mutual authentication is established, transmitting, to said data storage device, by said data recording device, a set of session-key-used CBC-mode-processing keys which are generated by executing, based on a session key generated in the mutual authentication, encryption processing in the CBC mode on said set of keys applicable to encryption processing on pieces of data to be stored in the sectors;

decrypting, by said data storage device, said set of session-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the session key;

transmitting, to said data storage device, a set of

storage-key-used CBC-mode-processing keys which are generated by executing, based on a storage key unique to said data storage device, encryption processing in the CBC mode on the set of decrypted session-key-used CBC-mode-processing keys; and

generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys, the header information corresponding to the data to be stored in said data storage device.

7. A data playback method for a data processor comprising: a data storage device comprising cryptosystem means and a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which each have a predetermined data capacity; and a data playback device for playing back data which is received from said data storage device, said data playback method comprising the steps of:

executing mutual authentication processing between said data storage device and said data playback device;

when the mutual authentication is established, transmitting, from said data playback device to said data storage device, a set of storage-key-used CBC-mode-processing keys which is included in the header information

of data stored in said data storage area and which is generated by executing encryption processing in the CBC mode using a storage key unique to said data storage device;

decrypting, by said data storage device, the set of storage-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the storage key;

transmitting, by said data storage device, to said data playback device, a set of session-key-used CBC-mode-processing keys which are generated by executing, based on a session key generated in the mutual authentication, encryption processing in the CBC mode on the set of decrypted storage-key-used CBC-mode-processing keys; and

obtaining, by said data playback device, a set of keys for decrypting encrypted sector data which is stored in each of the sectors in said data storage area by decrypting, in the CBC mode, the session-key-used CBC-mode-processing keys by using the session key.

8. A program providing medium for providing a computer program which controls a computer system to execute data recording processing for a data processor comprising: a data storage device comprising cryptosystem means and a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which each have a predetermined data capacity; and a data recording device for

executing data storage processing by transmitting data to said data storage device, said computer program comprising the steps of:

executing mutual authentication processing between said data storage device and said data recording device;

when the mutual authentication is established, transmitting, to said data storage device, by said data recording device, a set of session-key-used CBC-mode-processing keys which are generated by executing, based on a session key generated in the mutual authentication, encryption processing in the CBC mode on said set of keys applicable to encryption processing on pieces of data to be stored in the sectors;

decrypting, by said data storage device, said set of session-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the session key;

transmitting, to said data storage device, a set of storage-key-used CBC-mode-processing keys which are generated by executing, based on a storage key unique to said data storage device, encryption processing in the CBC mode on the set of decrypted session-key-used CBC-mode-processing keys; and

generating, by said data recording device, header information including as a component the received set of storage-key-used CBC-mode-processing keys, the header

information corresponding to the data to be stored in said data storage device.

9. A program providing medium for providing a computer program which controls a computer system to execute data playback processing for a data processor comprising: a data storage device comprising cryptosystem means and a data storage area consisting of a plurality of blocks, each of which consists of a plurality of sectors which each have a predetermined data capacity; and a data playback device for playing back data which is received from said data storage device; said computer program comprising the steps of:

executing mutual authentication processing between said data storage device and said data playback device;

when the mutual authentication is established, transmitting, from said data playback device to said data storage device, a set of storage-key-used CBC-mode-processing keys which is included in the header information of data stored in said data storage area and which is generated by executing encryption processing in the CBC mode using a storage key unique to said data storage device;

decrypting, by said data storage device, the set of storage-key-used CBC-mode-processing keys by performing decryption in the CBC mode using the storage key;

transmitting, by said data storage device, to said data

playback device, a set of session-key-used CBC-mode-processing keys which are generated by executing, based on a session key generated in the mutual authentication, encryption processing in the CBC mode on the set of decrypted storage-key-used CBC-mode-processing keys; and

obtaining, by said data playback device, a set of keys for decrypting encrypted sector data which is stored in each of the sectors in said data storage area by decrypting, in the CBC mode, the session-key-used CBC-mode-processing keys by using the session key.